China’s Position on the Sony Attack: Implications for the U.S. Response

by

Jordan Wilson
Research Fellow, Security and Foreign Affairs

Disclaimer: This paper is the product of professional research performed by staff of the U.S.-China Economic and Security Review Commission, and was prepared at the request of the Commission to support its deliberations. Posting of the report to the Commission’s website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 108-7. However, the public release of this document does not necessarily imply an endorsement by the Commission, any individual Commissioner, or the Commission’s other professional staff, of the views or conclusions expressed in this staff research report.

The author thanks Richard Bejtlich and Jon Lindsay for their review of early drafts. These experts do not necessarily agree with or endorse the staff report’s assessments and statements contained herein, and any errors should be attributed to the author.
Background

In late November 2014, Sony Pictures Entertainment confirmed it was the victim of a cyber attack that crippled its networks and stole large quantities of personal and commercial data. On December 19, the U.S. Federal Bureau of Investigation (FBI) publicly identified North Korea as responsible for these crimes, describing the attack as “destructive” and “coercive” in nature. President Obama pledged the United States would respond “proportionately” and “in a place and time and manner that we choose.” On January 2, 2015, the United States imposed financial sanctions on North Korea’s arms industry as a “first step in retaliation.” Analysts and news media have suggested further steps could include listing North Korea as a state sponsor of terrorism, bringing down its propaganda websites, and targeting its computer hardware, with a kinetic response termed “the remotest of possibilities.”

U.S. officials reached out to China’s government following this attribution in an effort to “share information,” “express our concerns,” and “ask for their cooperation,” as stated by one representative. The United States reportedly asked specifically for assistance in a “blocking action” to eliminate North Korea’s ability to carry out future attacks, as Chinese state-owned enterprise China Unicom is a crucial conduit for nearly all of the regime’s telecommunications. Beijing has yet to publicly respond to the U.S. overture or officially acknowledge North Korean involvement, stating only that China “is against all forms of cyber attacks,” including those launched by a state “using facilities beyond its own national borders against a third country.”

As China has received attention as a potential factor in this attack, is in a unique position to influence North Korea, and is a key player in the development of international norms in cyberspace, its reactions to U.S. decisions on these matters are of particular interest.

Was China Involved in the Attack against Sony?

President Obama said on December 20 the U.S. had found “no indication that North Korea was acting in conjunction with another country.” Some analysts have suggested, however, that China could have played a role in the attack, but the Administration has avoided public accusations for diplomatic reasons. Arguments for China’s involvement have largely drawn on its physical proximity to North Korea’s cyber infrastructure as well as political ties to its leadership; one U.S. senator made the case that carrying out an operation of this size required China “being involved or at least knowing about it,” a statement swiftly criticized by China’s government.

Other sources suggest the Sony attack could have been routed through Chinese servers or that a network of as many as 1,000 North Korean hackers operating in China could have played a role, particularly the “Bureau 121” group reportedly working out of North Korean-owned locations in Shenyang.

None of these assertions has been accompanied by substantive evidence of knowledge or assistance on the part of China’s government, however. Proximity is insufficient to prove complicity, as reports show the

---

* North Korea experienced recurring Internet failures over several days beginning December 22, 2014. Some have speculated the outages were the result of a U.S. cyber attack, but to date there has been no evidence to support this claim. Former director of operations at U.S. Cyber Command Maj. Gen. Brett Williams, USAF (Retd.) has stated it is “unlikely this was the result of U.S. actions,” as it was not a “proportionate response” as promised, and the United States would likely use a more sophisticated and targeted approach to impact the North Korean leadership directly. Interview with Lawrence O’Donnell, MSNBC, Television, December 22, 2014. http://www.msnbc.com/the-last-word/watch/what-s-behind-north-korean-internet-outage--376176707647.

† According to Richard Bejtlich, Chief Security Strategist at FireEye, Inc., the presence of these units in China could constitute “state-ignored” responsibility if China’s government knowingly allowed North Korean hackers to operate
Sony attack was routed through servers in Bolivia, Italy, the United States, and five other countries as well.17 Furthermore, evidence indicates North Korea is capable of having conducted the operation on its own; its cyber forces have benefited from a surge in investment and training in recent years,18 and previously developed a similar but more rudimentary malware called DarkSeoul, used to attack South Korea in 2013.19 FBI Director James Comey referred to “clear links” to this malware, as well as numerous other lines of evidence indicating North Korea’s responsibility, in detailed remarks given on January 7.20

Will China Assist the U.S. Response?

It is unlikely China will cooperate with U.S. government actions against North Korea, based on three factors:

- First, U.S.-China cyber cooperation is currently at a low point, marked by China’s suspension of the “U.S.-China Cyber Working Group” in May 2014 in response to the FBI’s indictment of five People’s Liberation Army officers for cyber espionage.21 Recent efforts to restart dialogue on the subject have proven unsuccessful.22 China considers the United States’ current stance to be hypocritical and threatening to its interests, and has used information on U.S. cyber activities from recent intelligence leaks to justify avoiding collaboration and to build traction with other like-minded nations.23 Given this atmosphere, China is extremely unlikely to assist the United States with a defining response in the cyber domain, particularly in such a politically-charged matter.

- Second, China to date has withheld judgment on whether North Korea was involved in the attack at all,24 and implied the FBI’s statement offers insufficient evidence to substantiate the U.S. claim.25 This is consistent with China’s refusal to assign blame for North Korea’s provocative actions in the past, including the sinking of a South Korean naval vessel and bombardment of a South Korean island in 2010,26 indicating it probably will take the same course in this case.

- Finally, China has actively censored reports on the cyber attack domestically,27 limiting its citizens’ access to the flood of media output detailing North Korea’s crimes. This would be an unlikely course of action to take if China were preparing to condemn or act against North Korea.

How Would China React to a U.S. Cyber Operation against North Korea?

In the case of a clear, attributable counterattack in cyberspace by the United States against North Korea, China most likely would respond with strong condemnation through official channels. Two considerations support this assumption:

- First, in the current contentious atmosphere of bilateral cyber relations, China is better able to defend its stance by condemning a unilateral move by the U.S. to define boundaries in this domain than by acquiescing to or supporting it. Affirming the “redline” drawn by U.S. retaliation would do harm to China’s position, as it would have had no input into the process of the line’s establishment and has found little common ground with the United States on setting such boundaries in the past.28

---


* This refers to North Korea’s use of either internal units or third party criminal groups to carry out the attack. The public FBI statement refers to the North Korean government’s “responsibility” and does not distinguish between these types of forces. For practical purposes such as identifying North Korea’s intent and capability to launch such an operation, there is no difference.
Condemning the U.S. operation, on the other hand, would be a costless move, as it is not likely to undermine the dialogue further while the two sides have yet to even begin identifying areas of agreement.

- Second, while a “second strike” such as this would be unprecedented, China’s past responses to other U.S. actions in the cyber domain are informative. Chinese official statements and domestic scholarly and media articles have excoriated U.S. cyber deterrence policies, stating in one article the United States is “playing a dangerous game with cyber deterrence” and “militarizing cyberspace.” Responding to U.S. cyber attribution efforts, some have called these cases “typically fictitious” and accused the United States of being too quick to attribute “improper individual behaviors” to state actors. Revelations of U.S. acts of cyber espionage led to descriptions of the United States as “the biggest cyber villain in our age.” This theme suggests a similar response from Beijing in the case of an unmistakable U.S. cyber attack for deterrence purposes.

Could a Response Deter Future Chinese Cyber Operations against the U.S.?

Responsive action against North Korea in any form takes the United States into uncharted territory in the worldwide cyber domain. The Sony cyber attack is a new type of event, as conducting a cyber operation against a company for coercive purposes goes beyond traditionally subtle cyber espionage, yet falls short of an “act of war” that causes equivalent to a traditional military attack. As stated by a former White House cybersecurity advisor, the United States’ decision will “indelibly serve to influence future nation-state behavior.” The costs imposed will help determine whether actions in this gray zone between computer network exploitation and computer network attack, creating “harms between the concepts of war and peace” as termed by one analyst, are deterred in the future, not only from North Korea but from state and non-state actors worldwide.

Past U.S. responses such as the FBI indictment or official denunciations have in no way discouraged Chinese state-sponsored intrusions into government and industry networks thus far. This case provides a new opening, however, for the United States to solidify its declaratory policy, define what is acceptable, and potentially change the calculus of actors in this domain in regards to this new type of attack. It can take this action without incurring the costs of disrupting an already weakened cyber dialogue with China, in which finding common ground on such redlines has been highly challenging. Although typical cyber espionage activities would remain unaffected, should Chinese entities ever in the future contemplate similar “gray zone” cyber operations against U.S. industry networks for coercive purposes, the precedent set by the U.S. response to North Korea likely will influence their calculations.

Conclusion

China’s likely position on the Sony attack and the developing U.S. response is that of a nonaligned and disapproving third party. A forceful and unmistakable retaliation offers the United States the opportunity to define redlines and enhance its security in this challenging domain, while incurring few costs due to the current stalled state of U.S.-China dialogue on cyber issues.

---


